



Building effective cyber resilience:
investing in awareness
and behavior change

[AXELOS.com](https://www.axelos.com)

Who we are and what we do



CabinetOffice

CAPITA



The logo for RESILIA, featuring a stylized red and white 'R' icon to the left of the word 'RESILIA' in a bold, sans-serif font, with a 'TM' trademark symbol to the right.

Cyber Resilience is the ability for an organization to resist, respond and recover from attacks that will impact the critical information they require to succeed and do business.

It's the crime of our generation

“Cybersecurity is a serious corporate risk issue affecting virtually all levels of significant business activity. Boards should seek to approach cyber risk from an enterprise-wide standpoint. Ultimately, as one director put it: **“Cybersecurity is a human issue”**”

‘Cyber Risk Oversight for Boards’, National Association of Corporate Directors, Jan 2015

“...cybersecurity risk affects a company's bottom line. It can drive up costs and impact revenue. It can harm an organization's ability to innovate and to gain and maintain customers”

NIST Framework for Improving Critical Infrastructure Cybersecurity, February 2014

“Cybersecurity remains America's greatest threat...Widespread and basic knowledge of cybersecurity best practices will go a long way to mitigating the threat, even if perfect security is impossible”

James Clapper, Director of National Intelligence, February 2016

“I want to personally apologize to each of you for what has happened, as I know you expect us to protect your information. We will continue to do everything in our power to make our systems and security processes better and more secure, and hope that we can earn back your trust and confidence in Anthem”

Joseph R Swedish, President and CEO, Anthem Inc.

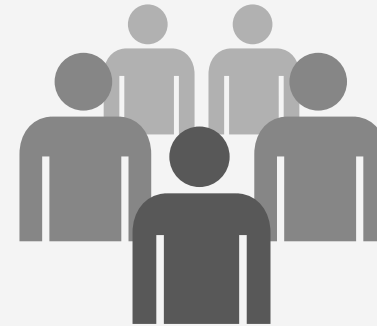
Everyone has a role to play

It's not just about bits and bytes...



90%...

...it's about behaviours



**...NEED TO INFLUENCE
AND ENABLE POSITIVE
CHANGE IN USER
BEHAVIOURS**

The agenda in the boardroom



Employee vulnerabilities - headlines

Clinic leaks HIV status of patients

Spoofed CEO email causes data breach at health care provider

Pentagon suffers data breach via spear phishing attack

Ubiquiti fraud: the \$46 million cyber crime

Fraudsters are using clever impersonation techniques to siphon millions from unprotected businesses

Sony hackers used phishing emails to breach company networks

Snapchat loses payroll information to phoul phisherpholk

Employee awareness - the facts

“Employee error is the most common reason for a data breach but fewer than half of in-house counsel said that mandatory awareness training exists at their company”

Association of Corporate Counsel (December 2015)

“The biggest barrier to effective cyber defense is low information security awareness among employees”

Survey of North American and European IT Security decision makers

“90% of all successful cyber-attacks rely on human vulnerability to succeed”

Verizon 2015 Data Breach Investigations Report

“60% of miscellaneous incidents were attributed to errors made by system administrators - prime actors responsible for a significant volume of breaches and records”

Verizon 2015 Data Beach Investigations Report

“Nearly two-thirds (62%) of staff interviewed said they thought their behaviour only has a low to moderate impact on security ”

CISCO Annual Security Report 2015 - interviewed 1000 members of staff

1 person can enable an attacker to compromise your systems and access your most valuable and commercially sensitive information.

Some racing certainties...

- Globalization, velocity of change, diverse cultural norms.
- More data breaches will involve the destruction of capability not just loss of data.
- Investors are increasingly concerned about resilience in determining value.
- The enemy will continue to be agile and industrialized...
- Compliance does not mean you are cyber resilient.
- **Managing cyber risks effectively is should be 'business as usual'.**
- **The human factor poses a massive cyber vulnerability for all.**
- **The Board will increasingly be held accountable and need to be ready to take informed action.**

...many are struggling to answer...



...what does good look like?

Why do security awareness programmes typically fail?



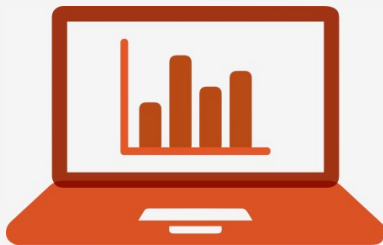
Reliance on checking the box



Failure to acknowledge that awareness is a unique discipline



Lack of engaging and appropriate materials



Metrics are not collected



Unreasonable expectations



Reliance on a single training exercise

Can e-learning really change behaviours?

YES.

But not in its current form - a one-off course, required once, designed once, delivered once, completed once and forgotten at once...

The Ebbinghaus 'forgetting curve':

- **40%** of information is forgotten in the first 20 minutes
- **More than half** of all information is forgotten after one hour
- **Only a fifth** of all information is remembered after one day



When does learning ‘stick’?

“Tell me and I forget,
Teach me and I remember,
Involve me and I learn.”

Benjamin Franklin

“Everybody can learn, just
not on the same day or in
the same way”

George Evans

Designing your campaign - remember!

PEOPLE PAY ATTENTION TO LEADERS

MEMORIES ARE FRAGILE

PEOPLE LEARN DIFFERENTLY

PEOPLE REMEMBER STORIES OVER FACTS

USE EVERY MEAN AT YOUR DISPOSAL

Our Awareness learning principles

Principle

On-going, regular learning

Adaptive & personalised

Engaging, competitive and fun

Measurable benefit

Summary and benefits

- Regular learning
- Short and concise
- Supporting updates and refreshers

- Suit individual learning preferences
- Content tailored to different skill levels
- Focus on the priority security issues

- Different learning styles and formats
- Ability to learn inside and outside work
- Play to the competitive element of games

- Tracking changing behaviours over time
- Qualitative and quantitative metrics
- Demonstrate value of investment


RESILIA Awareness Learning areas




Phishing




Social engineering



Online safety



Social media




BYOD



Removable media




Password safety



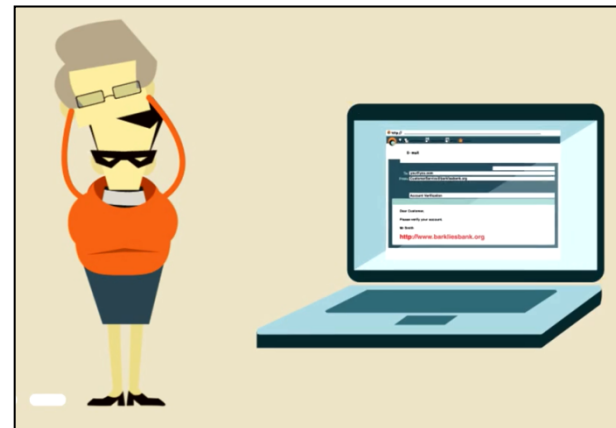
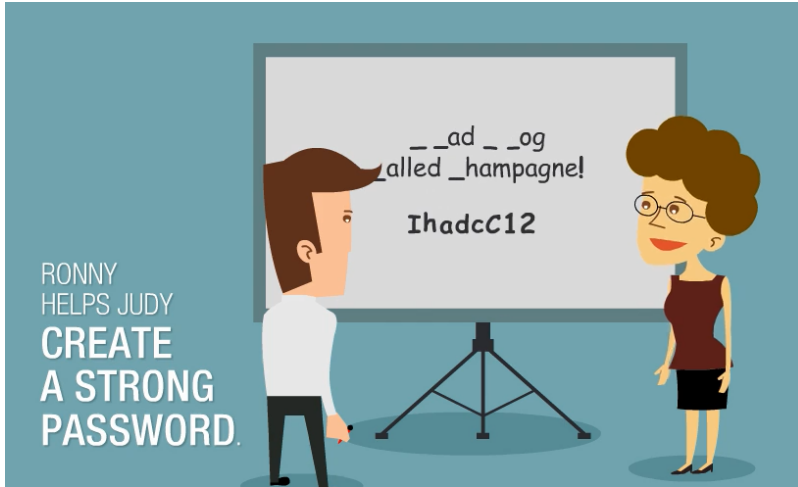
Personal information

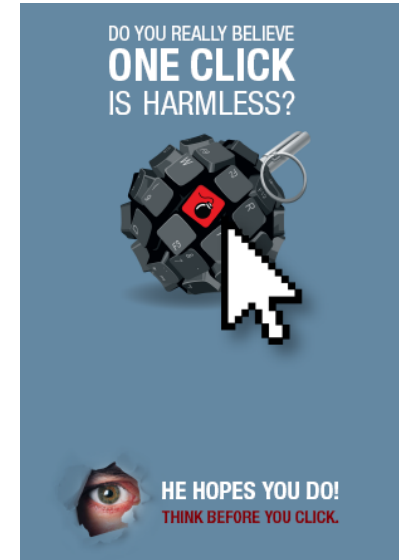


Information handling



Remote and mobile working

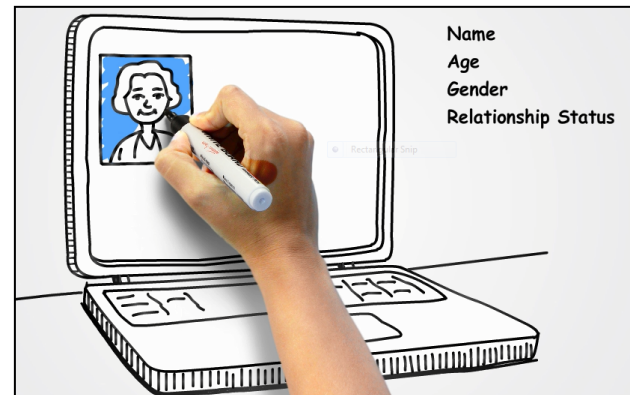




TIME LIMIT:
5:00

9 Increased Security Levels
You should consider upgrading your phishing templates if the company upgrades their security, or your attacks are not very effective. Let's head back to the mass email selector screen. Select the red building again.

Mark Logsdon
58 £0



A campaign template

DESIGN	CONCEIVE THE LEARNING AS A BRAND AND VISUALISE THE CAMPAIGN
PLAN	SCHEDULE THE LEARNING EVENTS OVER YOUR CAMPAIGN PERIOD
PUSH/ PULL	RELEASE COMMUNICATIONS AND LINK TO CONTENT
CURATE	FINE TUNE AND UPDATE THE CAMPAIGN PLATFORM
FEEDBACK	ASSESS WHAT'S WORKING AND ADJUST TACTICS AS REQUIRED

Summary

- Your people are your most effective security control but also potentially your greatest vulnerability.
- Traditional ‘once a year’ approaches to information security/cyber security awareness learning do not change behaviors.
- Understand your greatest risks and design your awareness campaign around protecting what most important to you.
- Keep the faith and keep learning - make the learning fun, engaging and interactive.
- Use stories and your own staff experiences to build interest, learning and new behaviors.

- And finally...JIM BAINES, CEO of Baines Packaging

Questions and observations?

Nick Wilding
Head of Cyber Resilience, AXELOS
E: nick.wilding@axelos.com

Rhonda MacLean
CEO, MacLean Risk Partners
E: rhonda.macleam@macleanriskpartners.com

